

27 Aug 2003

From: Deputy Assistant Judge Advocate General, Legal Assistance (Code 16)

Subj: IDENTITY THEFT (LAPA 24-03)

1. New Scam on the loose: In late July, the FBI and Federal Trade Commission reported the emergence of a new form of identity theft known as “phishing.” It works like this: unsolicited e-mails are sent to consumers from seemingly-official Internet Service Providers (ISPs) such as America Online, Earthlink, etc. These e-mails seem very real since they actually use the ISP official logo. The e-mails strongly encourage the recipient to click on a link provided in the e-mail—usually for some seemingly official purpose—for example, stating that there may be something wrong with the recipient’s account and it is on the verge of being closed. While the links appear to be to valid ISP websites, they are actually false websites run by the scammer. These false websites then ask the user to supply personal information including name, address, generic billing information, and other personal data.

2. Get the word out: 1) Servicemembers should NEVER click on links in e-mails that ask for personal information or claim that accounts will be closed if they do not respond immediately; 2) if they have a question about their account, they should call their ISP by phone to determine if a genuine issue exists regarding their account—obviously not using e-mail or phone contact information provided from the questionable e-mail itself; 3) they should always look for the “lock” symbol on their internet browser that accompanies secure websites requesting personal, sensitive information—this is the industry standard indicating the presence of security procedures protecting the user; 4) they should immediately report the receipt of such e-mail to law enforcement agencies in their area and to their local NLSO; and 5) they should file a complaint with the Military Sentinel database at www.consumer.gov/military.

3. Battling Identity Theft in general: We are all at risk for identity theft. Whether our personal information is gained through methods like “phishing,” taken out of our trash or mailbox, taken off a credit card receipt we leave at a restaurant, stolen from a credit card company’s computer database by illegal hacking, or gained by losing our wallet/purse—the risk is real. What should you do?

Some general guidance:

Make a photocopy of the contents of your wallet—all credit cards, driver’s license, etc., and *store this information in a safe place like a locked safe or safe deposit box*. If a credit card, your wallet, or your purse is lost or stolen, use this photocopied information to contact all the necessary credit card companies, state departments of motor vehicles, and any other agencies

immediately. Contact local law enforcement if you believe these items were stolen or as soon as you think identity theft has occurred.

Contact the three main credit bureaus—let them know that your wallet, purse, or credit card was stolen or misplaced, or alert them if you believe identity theft has occurred. Request that they not respond to any credit inquiries until further notice and that they contact you personally when an inquiry has been made for your credit information. Also request a copy of your credit report—you can obtain one free copy of your credit report each year, otherwise, there may be a minimal charge. The credit bureaus can be contacted as follows: Equifax at www.equifax.com; Transunion at www.transunion.com; and Experian at www.experian.com.

If you are tracking an identity theft situation, obtain a copy of your credit report every 2-3 months, notifying all unfamiliar companies named in the report of the fraud that has occurred in your name. If you believe identity theft has occurred, contact your bank and any other financial institutions with which you do business immediately—alert them to your situation and work with their security departments to protect existing accounts. Obtain a copy of your credit report annually even when you haven't lost a card or fear your identity has been stolen—it's a good way to check on the accuracy of your credit report and to stay on top of any issues that may develop (some people aren't aware that their identity has been stolen until they review their credit report). Do it the same time every year—perhaps after the New Year, or around your birthday for consistency and so it's easy to remember.

Stay vigilant to battle identity theft—don't think that it can't happen to you. Remember, even if you are extremely careful with your own affairs and personal information, including shredding all bills or receipts before throwing them away, etc., that doesn't mean that a financial institution that has your information can't be hacked or broken into!

4. If you have questions or need assistance concerning identity theft, contact LT Deidra Radel at radeldm@jag.navy.mil or call (202) 685-4641, DSN 325-4641.

V/r,

J. S. HEROLD